

特開平 10 - 107832

(43) 公開日 平成10年(1998)4月24日

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 12/54

H 0 4 L 11/20 1 0 1 B

12/58

G 0 6 F 13/00 3 5 1 G

G 0 6 F 13/00 3 5 1

G 0 9 C 1/00 6 6 0 G

G 0 9 C 1/00 6 6 0

H 0 4 L 9/00 6 4 1

H 0 4 L 9/14

11/18

審査請求 未請求 請求項の数 5

O L

(全 10 頁)

最終頁に続く

(21) 出願番号 特願平8-253599

(71) 出願人 000233055

(22) 出願日 平成8年(1996)9月25日

日立ソフトウェアエンジニアリング株式会
社

神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 鮫島 吉喜

神奈川県横浜市中区尾上町6丁目81番地

日立ソフトウェアエンジニアリング株式会
社内

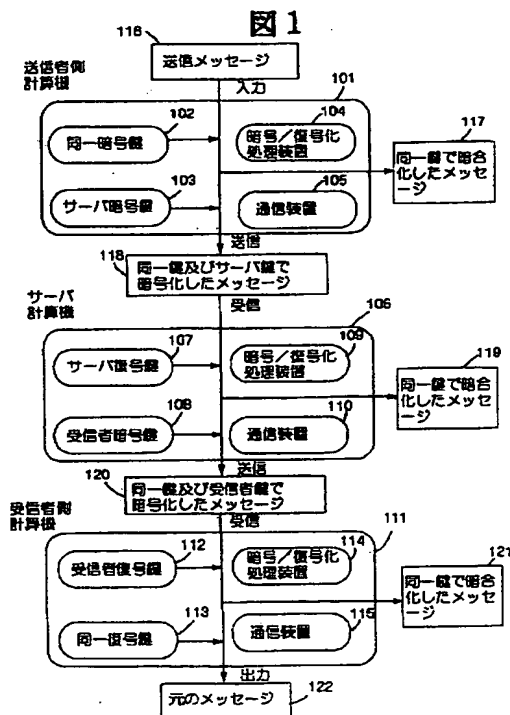
(74) 代理人 弁理士 秋田 収喜

(54) 【発明の名称】 暗号同報メールシステム

(57) 【要約】

【課題】 正規のメンバであった者がメーリングリストメンバから抜けた後に、メッセージを不法入手するのを防止し、セキュリティ上の向上を図る。

【解決手段】 送信者はメンバの持っている同一鍵で、メッセージを暗号化し、さらにメーリングリストサーバの鍵で暗号化して、サーバに送信する。サーバは受け取った鍵で復号し、次にメンバ（ここでは受信者を指す）各自が持っている復号鍵に対応する暗号鍵でそれぞれ暗号化し、メンバに送信する。2重に暗号化されたメッセージを受け取ったメンバである受信者は、まず、自分だけが持っている復号鍵で復号し、さらにメーリングリスト共通の復号鍵で復号する。



【特許請求の範囲】

【請求項1】 通信網によって相互接続された複数の送信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、送信者計算機が、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを暗号化した後、サーバ計算機だけでもしくはサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でさらにメッセージを暗号して、メールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で一度復号して、受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項2】 請求項1記載の暗号同報メールシステムにおいて、メールサーバ計算機が一度復号した後、サーバ計算機だけでもしくはサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージを暗号して、各受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項3】 請求項2記載の暗号同報メールシステムにおいて、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを直接暗号するのではなく、メッセージごとにメッセージ暗号鍵とメッセージ復号鍵を生成し、このメッセージ暗号鍵でメッセージを暗号し、メッセージ復号鍵をメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いて暗号化することを特徴とする暗号同報メールシステム。

【請求項4】 請求項3記載の暗号同報メールシステムにおいて、送信者計算機がメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージ復号鍵を暗号した後、サーバ計算機だけでもしくはサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵をさらに暗号して、暗号したメッセージとメッセージ復号鍵をメールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で暗号したメッセージ復号鍵を一度復号して、暗号したメッセージとメッセージ復号鍵を受信者計算機に送信することを特徴とする暗号同報メールシステム。

【請求項5】 請求項4記載の暗号同報メールシステムにおいて、メールサーバ計算機が暗号したメッセージ復号鍵を一度復号した後、サーバ計算機だけでもしくはサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵を暗号して、各受信者計算機に暗号したメッセージとメッセージ復号鍵を送信することを特徴とする暗号同報メールシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、電子メールシステムの中にある同じ内容のメッセージを複数の人に同報送信する、いわゆる同報メールもしくはメーリングリストサービスに係わる暗号同報メールシステムに関する。

【0002】

【従来の技術】 メーリングリストで暗号機能を実現するには、従来、3つの方法が知られている。第1の方法は、メーリングリストのメンバに同一の復号鍵を配布し、この復号鍵に対応する暗号鍵を用いてメッセージを暗号化して送信する方法である。

【0003】 第2の方法は、それぞれのメンバが復号鍵を持ち、送信者がそれぞれのメンバ受信者の復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【0004】 第3の方法は、それぞれのメンバが復号鍵を持ち、メーリングリストサーバメーリングリスト管理プログラムがそれぞれのメンバの復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【0005】

【発明が解決しようとする課題】 前記従来技術には以下のような問題点が挙げられる。

【0006】 前記第1の方法には、メーリングリストメンバが減った場合に問題が起こる。つまり、正規のメンバであった者が、メーリングリストメンバから抜けた後に、ネットワークを盗聴するなどしてメッセージを不法入手し、持っている復号鍵を使って暗号化されたメッセージを復号することができてしまう。これを防ぐためには、メンバが減る度に全てのメンバの鍵を交換する必要がおきてしまい、時間およびコストがかかってしまう。

【0007】 第2の方法では、全ての送信者が全てのメンバの暗号鍵をもっている必要があることに問題がある。例えば、メンバの増減や鍵の交換があると、その度に全ての送信者が自分が保有するメンバの構成を更新したりメンバの鍵を更新する必要があり、第1の方法と同様にコストがかかる。

【0008】 第3の方法では、本来メンバには含まれないメーリングリストサーバが、そして結果的にはサーバの管理者がメッセージ本体にアクセスすることができ、セキュリティ上の問題が生じる。

【0009】 本発明の目的は、これらの問題を解決する暗号同報メールシステムを提供することである。

【0010】

【課題を解決するための手段】 本発明は、メーリングリストサーバを用い、メッセージを二重に暗号することで課題を解決する。暗号に用いる鍵として、メンバそれぞれの鍵、メーリングリストサーバの鍵、メンバ共通の鍵同一鍵を用いる。鍵には暗号に使う鍵と復号に使う鍵の2種類がある。公開鍵暗号方式では、暗号鍵と復号鍵は別の鍵であり、暗号鍵は送信者を含め誰でもアクセスでき公開鍵と呼ばれ、復号鍵は受信者のみアクセスでき個人鍵と呼ばれる。対称鍵暗号方式では、2つの鍵は同一であり秘密鍵と呼ばれることが多い。

【0011】

【発明の実施の形態】 以下、図面を用いて本発明の実施の形態を詳細に説明する。

【0012】図1は、本発明を適用したシステムの第1の実施形態を示すシステム構成図である。

【0013】101はメーリングリストの参加メンバーであり、メーリングリストにメッセージを送る送信者の計算機である。102は前記メーリングリストにメッセージを送る送信者の計算機101が記憶している、メーリングリストの全てのメンバーの計算機が持っている同一暗号鍵である。

【0014】103は、計算機101が記憶しており、メーリングリストの全てのメンバーの計算機が持っているサーバの暗号鍵である。104は、計算機101が備えており、同一暗号鍵102、サーバ暗号鍵103の鍵を使ってメッセージの暗号処理や復号処理を行う暗号/復号装置である。105は、計算機101が備えており、メッセージをネットワークへ送信する通信装置である。

【0015】106はメーリングリストのサーバ計算機である。107は、サーバ計算機106が記憶し、サーバ暗号鍵103に対応する復号鍵であり、サーバ計算機106だけが記憶している。108は、サーバ計算機106が記憶しており、メンバーそれぞれの固有の暗号鍵である。なお、メンバーの暗号鍵はメンバーの数だけある。

【0016】109はサーバ計算機106が備えており、サーバ復号鍵107、メンバー固有の暗号鍵108を使ってメッセージの暗号や復号を行う暗号/復号装置である。

【0017】110はサーバ計算機106に備えられており、メッセージをネットワークから受信したり、ネットワークへ送信したりする通信装置である。111はメーリングリストの参加メンバーであり、サーバ計算機から送られてきたメッセージを受け取る受信者の計算機である。

【0018】112は受信者計算機111が記憶しており、メンバー固有の暗号鍵112に対応する復号鍵であり、受信者計算機111だけが記憶している。112は受信者計算機111が記憶しており、メーリングリストの全てのメンバーが持っている同一暗号鍵102に対応する同一の復号鍵であり、メンバーの計算機だけが記憶している。114は受信者計算機111が備えており、復号鍵112、同一復号鍵113の鍵を使ってメッセージの暗号や復号を行う暗号/復号装置である。

【0019】114は受信者計算機111が備えており、メッセージをネットワークから受信する装置である。116は送信者が作成するメッセージを示す。117は送信者計算機の中で同一暗号鍵102と暗号/復号装置104を使ってメッセージ116を暗号化したメッセージである。

【0020】118はサーバ暗号鍵103と暗/復号装置104を使って暗号メッセージ117をさらに暗号化したメッセージであり、送信者計算機からサーバ計算機へ通信装置105を使いネットワークを経由して送信さ

れる。118は同一暗号鍵102とサーバ暗号鍵103の鍵を使い、二重に暗号化されている複合暗号メッセージである。

【0021】119はサーバ計算機の中でサーバ復号鍵107と暗号/復号装置109を使って暗号メッセージ118を復号化したメッセージであり、暗号メッセージ117と同一である。

【0022】120はメンバー固有の暗号鍵108と暗号/復号装置109を使って、暗号メッセージ119を暗号化したメッセージであり、サーバ計算機から受信者計算機へ通信装置110を使い、ネットワークを経由して送信される。

【0023】121はサーバ計算機の中で復号鍵112と暗号/復号装置114を使って暗号メッセージ120を復号化したメッセージであり、暗号メッセージ117、119と同一である。122はサーバ計算機の中で同一復号鍵113と暗号/復号装置114を使って暗号メッセージ121を復号、出力したメッセージで、メッセージ116と同一である。なお、本明細書の実施の形態および、図面において、送信者側計算機と受信者側計算機はそれぞれ、単数で開示しているのは説明上の都合であり、それぞれが複数あっても構わない。

【0024】以下、図2のフロー図にしたがって、具体的な処理を説明する。

【0025】ステップ201からステップ204までは、送信者計算機101の処理を示す。ステップ205からステップ208までは、サーバ計算機106の処理を示す。ステップ209からステップ212までは、受信者計算機111の処理を示す。

【0026】送信者がメーリングリスト宛のメッセージ116を作成し送信者計算機101に入力する(ステップ201)。送信者計算機101が同一暗号鍵102と暗号/復号装置104を用いて入力されたメッセージ116を暗号化し、同一鍵で暗号化したメッセージ117を生成する(ステップ202)。

【0027】送信者計算機101がサーバ暗号鍵103と暗号/復号装置104を用いて、同一鍵で暗号化したメッセージ117をさらに暗号化し、同一鍵およびサーバ鍵で暗号化したメッセージ118を生成する(ステップ203)。送信者計算機101が通信装置105を用いて、先に生成したメッセージ118をサーバ計算機106宛にネットワークを経由して送信する(ステップ204)。

【0028】送信者計算機101が送信した暗号メッセージ118をサーバ計算機106が、通信装置110を用いて受信する(ステップ205)。サーバ計算機106がサーバ復号鍵107と暗号/復号装置109を用いて受信したメッセージ118を復号し、同一鍵で暗号化したメッセージ119を生成する(ステップ206)。

【0029】サーバ計算機106が、受信者暗号鍵10

8と暗号/復号装置109を用いて同一鍵で暗号したメッセージ119を暗号化し、同一鍵および受信者鍵で暗号したメッセージ120を生成する(ステップ207)。

【0030】このステップ207の処理は受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号メッセージ120を生成する。

【0031】サーバ計算機106が通信装置110を用いて、先に生成したメッセージ120を受信者計算機111宛にネットワークを経由して、送信する(ステップ208)。このステップ208の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に対応するメッセージ120を送信する。

【0032】サーバ計算機106が送信した暗号メッセージ120を受信者計算機111が、通信装置115を用いて受信する(ステップ209)。受信者計算機111が受信者復号鍵112と暗号/復号装置114を用いて受信したメッセージ120を復号し、同一鍵で暗号したメッセージ121を生成する(ステップ210)。

【0033】受信者計算機111が同一復号鍵113と暗号/復号装置114を用いて同一鍵で暗号したメッセージ121を復号する(ステップ211)。そして、この復号したメッセージ112を受信者に対して、出力する(ステップ212)。

【0034】(実施の形態2)次に、図3、図4を用いて本発明の第2の実施形態を詳細に説明する。

【0035】図3は全体のシステム構成を示す。図3において、301はメーリングリストの参加メンバであり、メーリングリストにメッセージを送る送信者の計算機である。302は送信者計算機301が記憶しており、メーリングリストの全てのメンバの計算機が持っている同一の暗号鍵である。

【0036】303は送信者計算機301が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバの暗号鍵である。304は送信者計算機301が備えており、メッセージ鍵の生成及びメッセージ鍵302、303の鍵を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置である。305は送信者計算機301が備えており、メッセージや鍵をネットワークへ送信する装置である。

【0037】306はメーリングリストのサーバ計算機である。307はサーバ計算機306が記憶しており、サーバ暗号鍵303の暗号鍵に対応する復号鍵であり、サーバ計算機306の計算機だけが記憶している。308は、サーバ計算機306が記憶しており、メンバそれぞれの暗号鍵である。メンバの暗号鍵はメンバの数だけある。309は、サーバ計算機306が備えており、サーバ復号鍵307、受信者暗号鍵308の鍵を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置で

ある。310は、サーバ計算機306が備えており、メッセージや鍵をネットワークから受信したり、ネットワークへ送信する装置である。

【0038】311はメーリングリストの参加メンバであり、サーバ計算機から送られてきたメッセージを受け取る受信者の計算機である。312は受信者計算機311が記憶しており、受信者暗号鍵308に対応する復号鍵であり、受信者計算機311だけが記憶している。

【0039】鍵作成/暗号化/復号化処理装置304は受信者計算機311が記憶しており、メーリングリストの全てのメンバが持っている同一暗号鍵302に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。

【0040】314は受信者計算機311が備えており、受信者復号鍵312、鍵作成/暗号化/復号化処理装置304を使ってメッセージやメッセージ復号鍵の暗号や復号を行う装置である。

【0041】315は、受信者計算機311が備えており、メッセージや鍵をネットワークから受信する装置である。316は送信者が作成するメッセージを示す。317は鍵作成/暗号化/復号化処理装置304が生成したメッセージ復号鍵である。

【0042】318は発信者計算機の中で鍵作成/暗号化/復号化処理装置304が生成したメッセージ暗号鍵と鍵作成/暗号化/復号化処理装置304を使って送信メッセージ316を暗号化したメッセージである。319は同一暗号鍵302と鍵作成/暗号化/復号化処理装置304を使ってメッセージ復号鍵317を暗号化されたメッセージ復号鍵である。

【0043】320は暗号メッセージ318と同一であり、送信者計算機301からサーバ計算機306へ通信装置305を使い、ネットワークを経由して送信される。321はサーバ暗号鍵303と鍵作成/暗号化/復号化処理装置304を使って、メッセージ復号鍵319を暗号したメッセージ復号鍵であり、送信者計算機301からサーバ計算機306へ通信装置305を使い、ネットワークを経由して送信される。

【0044】メッセージ復号鍵321は同一暗号鍵302とサーバ暗号鍵303の鍵を使い、二重に暗号化されている。暗号化メッセージ322は暗号化メッセージ318、320と同一で受信した暗号メッセージである。323はサーバ計算機の中でサーバ復号鍵307と暗号復号化装置309を使って、メッセージ復号鍵321を復号したメッセージ復号鍵である。

【0045】324は暗号化メッセージ318、320、322と同一であり、サーバ計算機306から受信者計算機311通信装置310を使い、ネットワークを経由して送信される。

【0046】325は受信者暗号鍵308と暗号復号装置309を使って、メッセージ復号鍵323を暗号化し

たメッセージ復号鍵であり、サーバ計算機306から受信者計算機311へ通信装置310を使い、ネットワークを経由して送信される。

【0047】326は暗号化メッセージ318、320、322、322と同一であり、受信した暗号メッセージである。326はサーバ計算機の中で受信者復号鍵312と暗号復号装置314を使ってメッセージ復号鍵325を復号したメッセージ復号鍵である。

【0048】328は同一復号鍵313と暗号復号装置314を使って、メッセージ復号鍵327を復号したメッセージ復号鍵で、メッセージ復号鍵317と同一である。

【0049】330はサーバ計算機の中でメッセージ復号鍵328と暗号復号装置314を使って、暗号化メッセージ326を復号、出力したメッセージで、送信メッセージ316と同一である。

【0050】以下、図4のフロー図にしたがって、処理を説明する。

【0051】ステップ401から406までは、送信者計算機301の処理を示す。ステップ407から410までは、サーバ計算機306の処理を示す。ステップ411から415までは、受信者計算機311の処理を示す。

【0052】送信者がメーリングリスト宛のメッセージ316を作成し、送信者計算機301に入力する（ステップ401）。送信者計算機301が鍵生成／暗復号装置304を使ってメッセージ暗号鍵とメッセージ復号鍵317を生成する（ステップ402）。

【0053】送信者計算機301が先に生成したメッセージ暗号鍵と鍵生成／暗復号装置304を用いて入力された送信メッセージ316を暗号化し、メッセージ鍵で暗号したメッセージ318を生成する（ステップ403）。

【0054】送信者計算機301が同一暗号鍵302と鍵作成／暗号化／復号化処理装置304を用いてメッセージ復号鍵317を暗号化し、同一鍵で暗号したメッセージ復号鍵319を生成する（ステップ404）。

【0055】送信者計算機301がサーバ暗号鍵303と鍵作成／暗号化／復号化処理装置304を用いて同一鍵で暗号化したメッセージ復号鍵319をさらに暗号化し、同一鍵およびサーバ鍵で暗号したメッセージ復号鍵321を生成する（ステップ405）。

【0056】送信者計算機301が通信装置305を用いて、先に暗号したメッセージ318、320と同一と同一鍵およびサーバ鍵で暗号したメッセージ復号鍵321をサーバ計算機306宛にネットワークを経由して送信する（ステップ406）。

【0057】送信者計算機301が送信したメッセージ320とメッセージ復号鍵321をサーバ計算機サーバ計算機306が通信装置310を用いて、受信する（ス

テップ407）。

【0058】サーバ計算機306がサーバ復号鍵307と暗号／復号装置309を用いて、受信したメッセージ復号鍵321を復号し、同一鍵で暗号したメッセージ復号鍵323を生成する（ステップ408）。この時、暗号したメッセージ322はそのままである。

【0059】サーバ計算機306が、受信者暗号鍵308と暗号／復号装置309を用いて同一鍵で暗号したメッセージ復号鍵323を暗号化し、同一鍵および受信者鍵で暗号化したメッセージ復号鍵325を生成する（ステップ409）。このステップ409の処理は、受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号し、各受信者ごとに暗号したメッセージ復号鍵325を生成する。

【0060】サーバ計算機306が通信装置310を用いて、先に生成したメッセージ復号鍵325と暗号したメッセージ（322、324と同一）を受信者計算機311宛にネットワークを経由して送信する（ステップ410）。このステップ410の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に暗号したメッセージ324と受信者に対応するメッセージ復号鍵325を送信する。

【0061】サーバ計算機306が送信した暗号したメッセージ324とメッセージ復号鍵325を受信者計算機311が通信装置315を用いて受信する（ステップ411）。

【0062】受信者計算機311が受信者復号鍵312と暗号／復号装置314を用いて受信したメッセージ復号鍵349を復号し、同一鍵で暗号したメッセージ復号鍵327を生成する（ステップ412）。この時、暗号したメッセージ326はそのままである。

【0063】受信者計算機311が受信者復号鍵312と暗号／復号装置314を用いて同一鍵で暗号したメッセージ復号鍵327を復号し、元のメッセージ復号鍵317と同じメッセージ復号鍵328を得る（ステップ413）。暗号化したメッセージ3263をメッセージ復号鍵328と暗号／復号装置315を用いて復号する（ステップ414）。この復号したメッセージ330を受信者に対して出力する（ステップ415）。

【0064】

【発明の効果】本発明によると、送信者からサーバに送られるメッセージもしくはメッセージ復号鍵は、メンバが共通に持っている鍵で暗号され、さらにサーバの鍵で暗号されているので、サーバだけが復号できる。

【0065】また、メーリングリストから抜けてしまったメンバはたとえ、メンバ同一の復号鍵を持っていてもアクセスできない。メンバが減った時には、メールサーバ計算機内部の変更だけで済み、メンバ送受信者の計算機の変更が不要になる。

【0066】また、メッセージもしくはメッセージ復号鍵はメンバ計算機だけが復号できる同一鍵で暗号されているのでメールサーバ計算機はアクセスすることができず、第三者による盗聴、情報の漏洩を防ぐことができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示すシステム構成図である。

【図2】本発明の第1の施の形態の処理を示すフローチャートである。

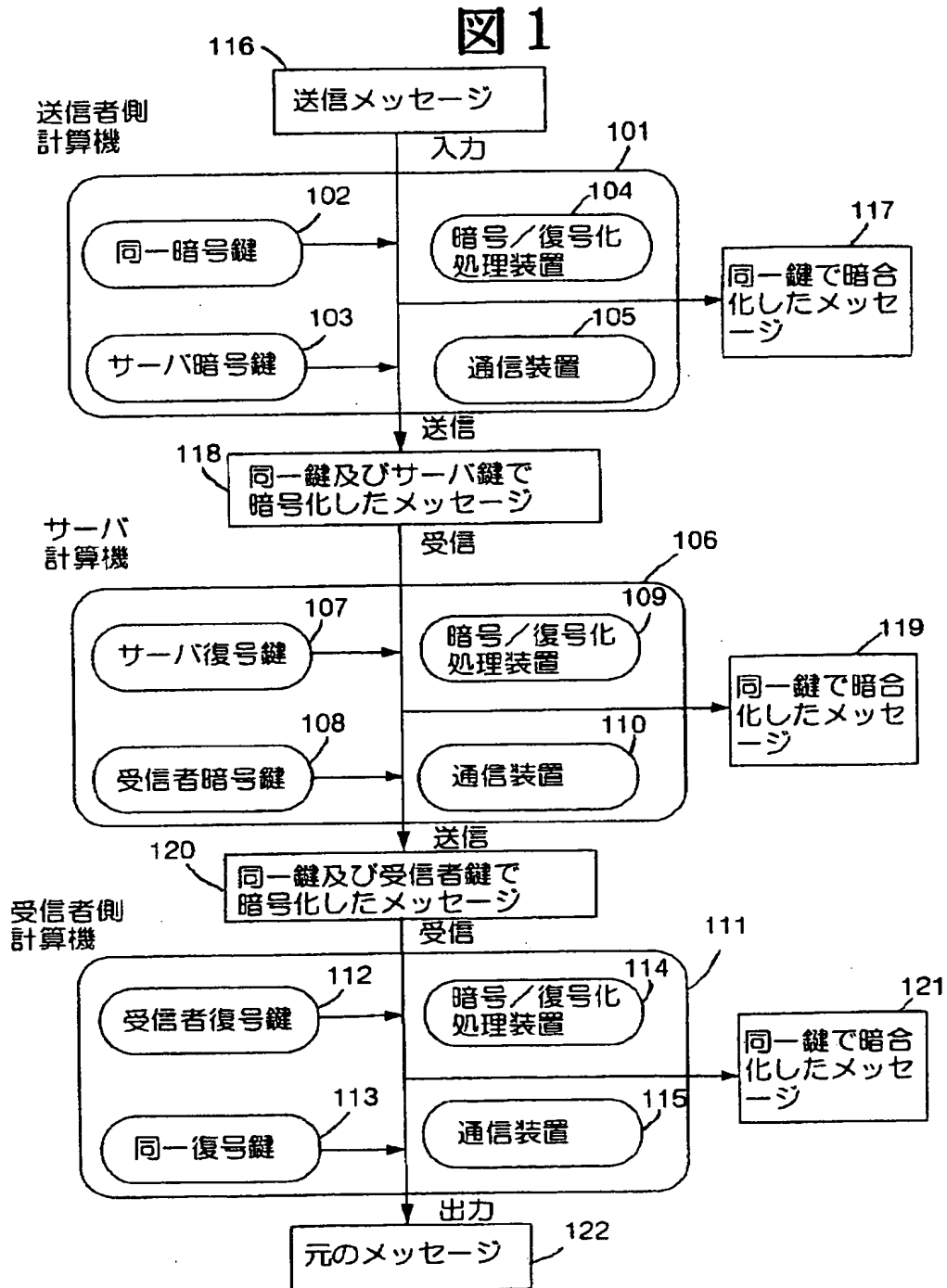
【図3】本発明の第2の実施形態を示すシステム構成図である。

【図4】本発明の第2の実施の形態の処理を示すフローチャートである。

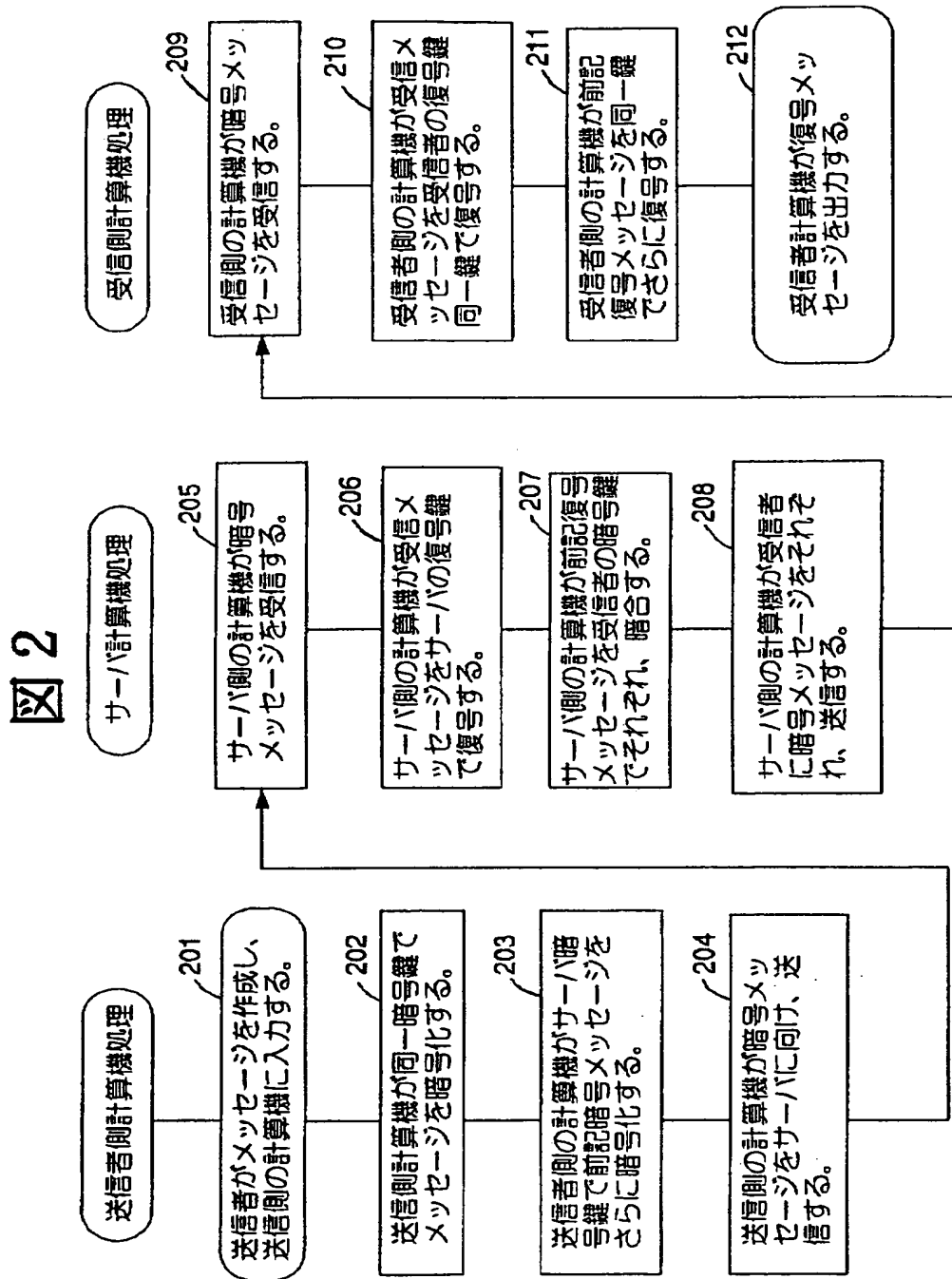
【符号の説明】

102…同一暗号鍵、103…サーバ暗号鍵、104, 109, 114…暗号/復号化処理装置、105, 110, 115…通信装置、107…サーバ復号鍵、108…受信者暗号鍵、112…受信者復号鍵、113…同一復号鍵。

【図1】



【図2】



【図3】

図 3

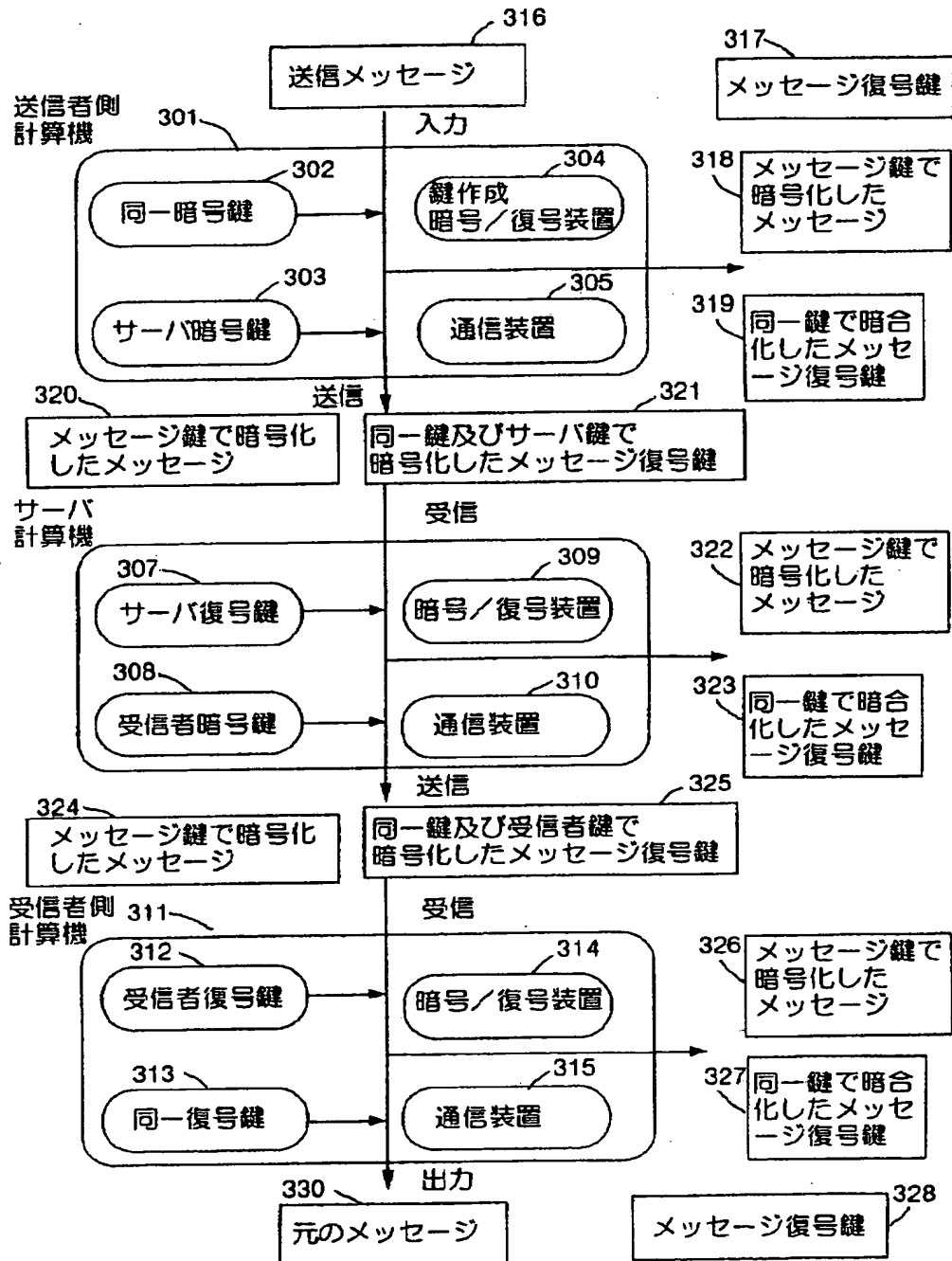
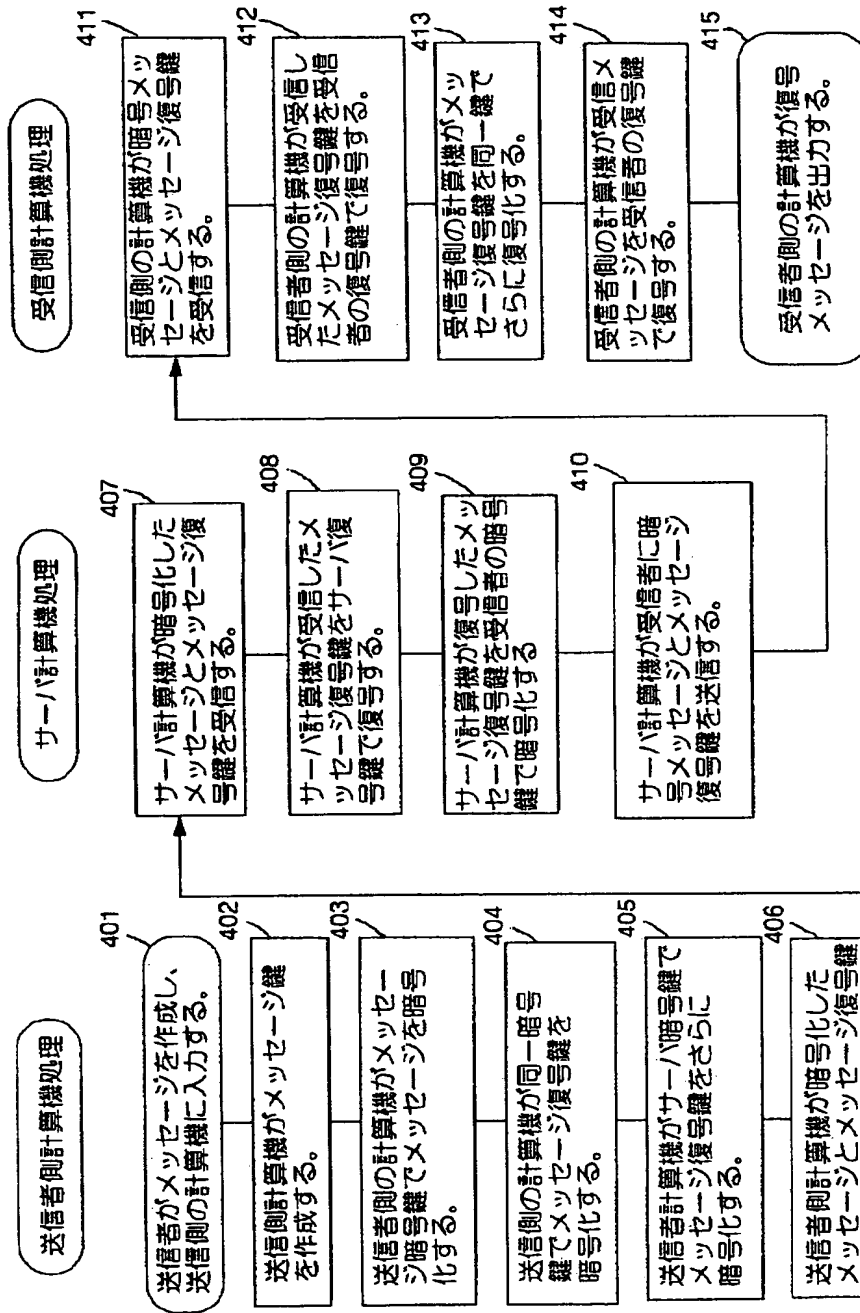


図4



【図4】

フロントページの続き

(51) Int. Cl. ⁶

H 0 4 L 12/18

識別記号

F I

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 7 部門第 3 区分

【発行日】平成 11 年（1999）11 月 30 日

【公開番号】特開平 10—107832

【公開日】平成 10 年（1998）4 月 24 日

【年通号数】公開特許公報 10—1079

【出願番号】特願平 8—253599

【国際特許分類第 6 版】

H04L 12/54
12/58
G06F 13/00 351
G09C 1/00 660
H04L 9/14
12/18

【F I】

H04L 11/20 101 B
G06F 13/00 351 G
G09C 1/00 660 G
H04L 9/00 641
11/18

【手続補正書】

【提出日】平成 11 年 3 月 23 日

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正内容】

【書類名】明細書

【発明の名称】暗号同報メールシステムの同報通信方法

【特許請求の範囲】

【請求項 1】 通信網によって相互接続された複数の送受信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、送信者計算機が、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを暗号化した後、前記メールサーバ計算機だけもしくはメールサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でさらにメッセージを暗号化して、メールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で一度復号して、受信者計算機に送信することを特徴とする暗号同報メールシステムの同報通信方法。

【請求項 2】 請求項 1 記載の暗号同報メールシステムにおいて、メールサーバ計算機が一度復号した後、受信者計算機だけもしくはメールサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージを暗号化して、各受信者計算機に送信することを

特徴とする暗号同報メールシステムの同報通信方法。

【請求項 3】 請求項 1 記載の暗号同報メールシステムにおいて、メールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージを直接暗号化ではなく、メッセージごとにメッセージ暗号鍵とメッセージ復号鍵を生成し、このメッセージ暗号鍵でメッセージを暗号化し、メッセージ復号鍵をメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いて暗号化することを特徴とする暗号同報メールシステムの同報通信方法。

【請求項 4】 通信網によって相互接続された複数の送受信者の計算機と同報メール機能を有するメールサーバ計算機からなる同報メールシステムにおいて、送信者計算機がメールの受信者計算機が記憶している復号鍵に対応する暗号鍵を用いてメッセージ復号鍵を暗号化した後、メールサーバ計算機だけもしくはメールサーバ計算機と送信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵をさらに暗号化して、暗号化したメッセージとメッセージ復号鍵をメールサーバ計算機に送信し、メールサーバ計算機は、暗号鍵に対応する復号鍵で暗号化したメッセージ復号鍵を一度復号して、暗号化したメッセージとメッセージ復号鍵を受信者計算機に送信することを特徴とする暗号同報メールシステムの同報通信方法。

【請求項 5】 請求項 4 記載の暗号同報メールシステムにおいて、メールサーバ計算機が暗号したメッセージ復号鍵を一度復号した後、受信者計算機だけもしくはメー

ルサーバ計算機と各受信者計算機のみが記憶している復号鍵に対応する暗号鍵でメッセージ復号鍵を暗号して、各受信者計算機に暗号したメッセージとメッセージ復号鍵を送信することを特徴とする暗号同報メールシステムの同報通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子メールシステムにおいて同じ内容のメッセージを複数の人に同報送信する、いわゆる同報メールもしくはメーリングリストサービスに係わる暗号同報メールシステムの同報通信方法に関する。

【0002】

【従来の技術】メーリングリストで暗号機能を実現するには、従来、3つの方法が知られている。第1の方法は、メーリングリストのメンバに同一の復号鍵を配布し、この復号鍵に対応する暗号鍵を用いてメッセージを暗号化して送信する方法である。

【0003】第2の方法は、それぞれのメンバが復号鍵を持ち、送信者がそれぞれのメンバ受信者の復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【0004】第3の方法は、それぞれのメンバが復号鍵を持ち、メーリングリストサーバメーリングリスト管理プログラムがそれぞれのメンバの復号鍵に対応する暗号鍵を用いて暗号化して送る方法である。

【0005】

【発明が解決しようとする課題】前記従来技術には以下のような問題点が挙げられる。

【0006】前記第1の方法には、メーリングリストメンバが減った場合に問題が起こる。つまり、正規のメンバであった者が、メーリングリストメンバから抜けた後に、ネットワークを盗聴するなどしてメッセージを不法入手し、持っている復号鍵を使って暗号化されたメッセージを復号することができてしまう。これを防ぐためには、メンバが減る度に全てのメンバの鍵を交換する必要がおきてしまい、時間およびコストがかかってしまう。

【0007】第2の方法では、全ての送信者が全てのメンバの暗号鍵をもっている必要があることに問題がある。例えば、メンバの増減や鍵の交換があると、その度に全ての送信者が自分が保有するメンバの構成を更新したりメンバの鍵を更新する必要があり、第1の方法と同様にコストがかかる。

【0008】第3の方法では、本来メンバには含まれないメーリングリストサーバが、そして結果的にはサーバの管理者がメッセージ本体にアクセスすることができ、セキュリティ上の問題が生じる。

【0009】本発明の目的は、これらの問題を解決する暗号同報メールシステムの同報通信方法を提供することである。

【0010】

【課題を解決するための手段】本発明は、メーリングリストサーバを用い、メッセージを二重に暗号化することで課題を解決する。暗号に用いる鍵として、メンバそれぞれの鍵、メーリングリストサーバの鍵、メンバ共通の同一暗号鍵を用いる。鍵には暗号化に使う鍵と復号に使う鍵の2種類がある。公開鍵暗号方式では、暗号鍵と復号鍵は別の鍵であり、暗号鍵は送信者を含め誰でもアクセスでき公開鍵と呼ばれ、復号鍵は受信者のみアクセスでき個人鍵と呼ばれる。対称鍵暗号方式では、2つの鍵は同一であり秘密鍵と呼ばれることが多い。

【0011】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を詳細に説明する。

【0012】図1は、本発明を適用したシステムの第1の実施形態を示すシステム構成図である。

【0013】101はメーリングリストの参加メンバであり、メーリングリストにメッセージを送る送信者側の計算機（以下、送信者計算機と言う）である。102は前記メーリングリストにメッセージを送る送信者計算機101が記憶している、メーリングリストの全てのメンバの計算機が持っている同一暗号鍵である。

【0014】103は、送信者計算機101が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバの暗号鍵である。104は、送信者計算機101が備えており、同一暗号鍵102、サーバ暗号鍵103を使ってメッセージの暗号化処理や復号処理を行う暗号／復号化処理装置である。105は、計算機101が備えており、メッセージをネットワークへ送信する通信装置である。

【0015】106はメーリングリストのサーバ計算機である。107は、サーバ計算機106が記憶し、サーバ暗号鍵103に対応するサーバ復号鍵であり、サーバ計算機106だけが記憶している。108は、サーバ計算機106が記憶しており、メンバそれぞれの固有の受信者暗号鍵である。なお、メンバの受信者暗号鍵はメンバの数だけある。

【0016】109はサーバ計算機106が備えており、サーバ復号鍵107、メンバ固有の受信者暗号鍵108を使ってメッセージの暗号化や復号を行う暗号／復号化処理装置である。

【0017】110はサーバ計算機106に備えられており、メッセージをネットワークから受信したり、ネットワークへ送信したりする通信装置である。111はメーリングリストの参加メンバが使用し、サーバ計算機106から送られてきたメッセージを受け取る受信者側の計算機（以下、受信者計算機と言う）である。

【0018】112は受信者計算機111が記憶しており、メンバ固有の暗号鍵112に対応する受信者復号鍵であり、受信者計算機111だけが記憶している。112は受信者計算機111が記憶しており、メーリングリ

ストの全てのメンバが持っている同一暗号鍵102に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。114は受信者計算機111が備えており、復号鍵112、同一復号鍵113を使ってメッセージの暗号化や復号を行う暗号/復号化処理装置である。

【0019】115は受信者計算機111が備えており、メッセージをネットワークから受信する通信装置である。116は送信者が作成するメッセージを示す。117は送信者計算機101の中で同一暗号鍵102と暗号/復号化処理装置104を使ってメッセージ116を暗号化したメッセージである。

【0020】118はサーバ暗号鍵103と暗号/復号化処理装置104を使って暗号メッセージ117をさらに暗号化したメッセージであり、送信者計算機101からサーバ計算機106へ通信装置105を使いネットワークを経由して送信される。このメッセージ118は同一暗号鍵102とサーバ暗号鍵103を使い、二重に暗号化されている複合暗号メッセージである。

【0021】119はサーバ計算機の中でサーバ復号鍵107と暗号/復号化処理装置109を使って暗号メッセージ118を復号したメッセージであり、暗号メッセージ117と同一である。

【0022】120はメンバ固有の受信者暗号鍵108と暗号/復号化処理装置109を使って、暗号メッセージ119をさらに暗号化したメッセージ(すなわち、同一暗号鍵102および受信者暗号鍵108で暗号化したメッセージ)であり、サーバ計算機106から受信者計算機111へ通信装置110を使い、ネットワークを経由して送信される。

【0023】121は受信者計算機111の中で復号鍵112と暗号/復号化処理装置114を使って暗号メッセージ120を復号化したメッセージであり、暗号メッセージ117、119と同一である。122は受信者計算機111の中で同一復号鍵113と暗号/復号化処理装置114を使って暗号メッセージ121を復号して出力したメッセージであり、送信メッセージ116と同一である。なお、本明細書の実施の形態および、図面において、送信者側計算機101と受信者側計算機111はそれぞれ、単数で開示しているのは説明上の都合であり、それぞれが複数あっても構わない。

【0024】以下、図2のフロー図にしたがって、具体的な処理を説明する。

【0025】ステップ201からステップ204までは、送信者計算機101の処理を示す。ステップ205からステップ208までは、サーバ計算機106の処理を示す。ステップ209からステップ212までは、受信者計算機111の処理を示す。

【0026】送信者がメーリングリスト宛のメッセージ116を作成し送信者計算機101に入力する(ステップ201)。送信者計算機101が同一暗号鍵102と

暗号/復号化処理装置104を用いて、入力されたメッセージ116を暗号化し、同一暗号鍵102で暗号化したメッセージ117を生成する(ステップ202)。

【0027】送信者計算機101がサーバ暗号鍵103と暗号/復号化処理装置104を用いて、暗号メッセージ117をさらに暗号化し、同一暗号鍵102およびサーバ暗号鍵103で暗号化したメッセージ118を生成する(ステップ203)。送信者計算機101が通信装置105を用いて、先に生成したメッセージ118をサーバ計算機106宛にネットワークを経由して送信する(ステップ204)。

【0028】送信者計算機101が送信した暗号メッセージ118をサーバ計算機106が、通信装置110を用いて受信する(ステップ205)。サーバ計算機106がサーバ復号鍵107と暗号/復号化処理装置109を用いて、受信したメッセージ118を復号し、同一暗号鍵102で暗号化したメッセージ119を復元する(ステップ206)。

【0029】サーバ計算機106が、受信者暗号鍵108と暗号/復号化処理装置109を用いて、同一暗号鍵102で暗号化されているメッセージ119を受信者暗号鍵108によってさらに暗号化し、同一暗号鍵102および受信者暗号鍵108で暗号化したメッセージ120を生成する(ステップ207)。

【0030】このステップ207の処理は受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号メッセージ120を生成する。

【0031】サーバ計算機106が通信装置110を用いて、先に生成したメッセージ120を受信者計算機111宛にネットワークを経由して、送信する(ステップ208)。このステップ208の処理もそれぞれの受信者に対して繰り返す。つまり、それぞれの受信者の計算機に対応するメッセージ120を送信する。

【0032】サーバ計算機106が送信した暗号メッセージ120を受信者計算機111が、通信装置115を用いて受信する(ステップ209)。受信者計算機111が受信者復号鍵112と暗号/復号化処理装置114を用いて、受信したメッセージ120を復号し、同一暗号鍵102で暗号化されているメッセージ121を復元する(ステップ210)。

【0033】受信者計算機111が同一復号鍵113と暗号/復号化処理装置114を用いて、同一暗号鍵102で暗号化されているメッセージ121を復号する(ステップ211)。そして、この復号したメッセージ122を受信者に対して、出力する(ステップ212)。

【0034】(実施の形態2)次に、図3、図4を用いて本発明の第2の実施形態を詳細に説明する。

【0035】図3は全体のシステム構成を示す。図3において、301はメーリングリストの参加メンバであ

り、メーリングリストにメッセージを送る送信者の計算機である。302は送信者計算機301が記憶しており、メーリングリストの全てのメンバの計算機が持っている同一の暗号鍵である。

【0036】303は送信者計算機301が記憶しており、メーリングリストの全てのメンバの計算機が持っているサーバ計算機の暗号鍵である。304は送信者計算機301が備えており、メッセージ鍵の生成及びメッセージ暗号化用の鍵302、303を使ってメッセージやメッセージ鍵の暗号化や復号を行う鍵作成／暗号／復号装置である。305は送信者計算機301が備えており、メッセージや暗号化した鍵をネットワークへ送信する装置である。

【0037】306はメーリングリストのサーバ計算機である。307はサーバ計算機306が記憶しており、サーバ暗号鍵303に対応する復号鍵であり、サーバ計算機306の計算機だけが記憶している。308は、サーバ計算機306が記憶しており、メンバそれぞれの受信者暗号鍵である。メンバの受信者暗号鍵308はメンバの数だけある。309は、サーバ計算機306が備えており、サーバ復号鍵307、受信者暗号鍵308を使ってメッセージやメッセージ鍵の暗号化や復号を行う暗号／復号装置である。310は、サーバ計算機306が備えており、メッセージや暗号化した鍵をネットワークから受信したり、ネットワークへ送信する装置である。

【0038】311はメーリングリストの参加メンバであり、サーバ計算機306から送られてきたメッセージを受け取る受信者の計算機である。312は受信者計算機311が記憶しており、受信者暗号鍵308に対応する受信者復号鍵であり、受信者計算機311だけが記憶している。

【0039】313は、受信者計算機311が記憶しており、メーリングリストの全てのメンバが持っている同一暗号鍵302に対応する同一の復号鍵であり、メンバの計算機だけが記憶している。

【0040】314は受信者計算機311が備えており、受信者復号鍵312、同一復号鍵313を使ってメッセージやメッセージ鍵の暗号化や復号を行う暗号／復号装置である。

【0041】315は、受信者計算機311が備えており、メッセージや暗号化した鍵をネットワークから受信する通信装置である。316は送信者が作成するメッセージを示す。317は鍵作成／暗号／復号装置304が生成したメッセージ鍵である。

【0042】318は送信者計算機301の中で鍵作成／暗号／復号装置304が生成したメッセージ鍵317と、鍵作成／暗号／復号装置304を使って送信メッセージ316を暗号化したメッセージである。319は同一暗号鍵302と鍵作成／暗号／復号装置304を使ってメッセージ鍵317を暗号化したメッセージ鍵であ

る。

【0043】320は暗号メッセージ318と同一であり、送信者計算機301からサーバ計算機306へ通信装置305を使い、ネットワークを経由して送信される。321はサーバ暗号鍵303と鍵作成／暗号／復号装置304を使って、メッセージ鍵319を暗号化したメッセージ鍵（すなわち、メッセージ鍵317を同一暗号鍵302で暗号化し、さらにサーバ暗号鍵303で暗号化した鍵）であり、送信者計算機301からサーバ計算機306へ通信装置305を使い、ネットワークを経由して送信される。

【0044】メッセージ鍵321は同一暗号鍵302とサーバ暗号鍵303の鍵を使い、二重に暗号化されている。暗号化メッセージ322は暗号化メッセージ318、320と同一であり、受信した暗号メッセージである。323はサーバ計算機306の中でサーバ復号鍵307と暗号／復号装置309を使って、メッセージ鍵321を復号したメッセージ鍵（すなわち、同一暗号鍵302で暗号化したメッセージ鍵）である。

【0045】324は暗号化メッセージ318、320、322と同一であり、サーバ計算機306から受信者計算機311に対し通信装置310を使い、ネットワークを経由して送信される。

【0046】325は受信者暗号鍵308と暗号／復号装置309を使って、同一暗号鍵302で暗号化したメッセージ鍵323を受信者暗号鍵308によってさらに暗号化したメッセージ鍵であり、サーバ計算機306から受信者計算機311へ通信装置310を使い、ネットワークを経由して送信される。

【0047】326は暗号化メッセージ318、320、322、324と同一であり、受信した暗号メッセージである。327は受信者計算機311の中で受信者復号鍵312と暗号／復号装置314を使ってメッセージ鍵（同一暗号鍵と受信者暗号鍵で暗号化した鍵）325を復号したメッセージ鍵である。

【0048】328は同一復号鍵313と暗号／復号装置314を使って、同一暗号鍵で暗号化したメッセージ鍵327を同一復号鍵313で復号したメッセージ鍵で、メッセージ鍵317と同一である。

【0049】330はサーバ計算機306の中でメッセージ復号鍵328と暗号／復号装置314を使って、メッセージ鍵で暗号化したメッセージ326を復号し、出力したメッセージで、送信メッセージ316と同一である。

【0050】以下、図4のフロー図にしたがって、処理を説明する。

【0051】ステップ401から406までは、送信者計算機301の処理を示す。ステップ407から410までは、サーバ計算機306の処理を示す。ステップ411から415までは、受信者計算機311の処理を示す。

す。

【0052】送信者がメーリングリスト宛のメッセージ316を作成し、送信者計算機301に入力する（ステップ401）。送信者計算機301が鍵生成／暗号／復号装置304を使ってメッセージ鍵317を生成する（ステップ402）。

【0053】送信者計算機301が先に生成したメッセージ鍵317と鍵生成／暗号／復号装置304を用いて、入力された送信メッセージ316をメッセージ鍵317で暗号化し、メッセージ鍵317で暗号化したメッセージ318を生成する（ステップ403）。

【0054】送信者計算機301が同一暗号鍵302と鍵作成／暗号／復号装置304を用いて、メッセージ鍵317を暗号化し、同一暗号鍵302で暗号化したメッセージ鍵319を生成する（ステップ404）。

【0055】送信者計算機301がサーバ暗号鍵303と鍵作成／暗号／復号装置304を用いて、同一暗号鍵302で暗号化したメッセージ鍵319をサーバ暗号鍵303でさらに暗号化し、同一暗号鍵302およびサーバ暗号鍵303で暗号化したメッセージ鍵321を生成する（ステップ405）。

【0056】送信者計算機301が通信装置305を用いて、先に暗号化したメッセージ318と同一のメッセージ320と同一暗号鍵302およびサーバ暗号鍵303で暗号化したメッセージ鍵321をサーバ計算機306宛にネットワークを経由して送信する（ステップ406）。

【0057】送信者計算機301が送信したメッセージ320とメッセージ鍵321をサーバ計算機306が通信装置310を用いて、受信する（ステップ407）。

【0058】サーバ計算機306がサーバ復号鍵307と暗号／復号装置309を用いて、受信したメッセージ鍵321を復号し、同一暗号鍵302で暗号化されているメッセージ鍵323を復元する（ステップ408）。この時、暗号化したメッセージ322はそのままである。

【0059】サーバ計算機306が、受信者暗号鍵308と暗号／復号装置309を用いて同一暗号鍵302で暗号化したメッセージ鍵323を暗号化し、同一暗号鍵302および受信者暗号鍵308で暗号化したメッセージ鍵325を生成する（ステップ409）。このステップ409の処理は、受信者であるメーリングリストのメンバそれぞれに対して行う。つまり、それぞれの受信者の暗号鍵で暗号化し、各受信者ごとに暗号したメッセージ鍵325を生成する。

【0060】サーバ計算機306が通信装置310を用いて、先に生成したメッセージ鍵325と暗号化したメッセージ（322と同一）324を受信者計算機311宛にネットワークを経由して送信する（ステップ410）。このステップ410の処理もそれぞれの受信者に

対して繰り返す。つまり、それぞれの受信者の計算機に暗号したメッセージ324と受信者に対応するメッセージ鍵325を送信する。

【0061】サーバ計算機306が送信した暗号化されたメッセージ324とメッセージ鍵325を受信者計算機311が通信装置315を用いて受信する（ステップ411）。

【0062】受信者計算機311が受信者復号鍵312と暗号／復号装置314を用いて、受信したメッセージ鍵325を復号し、同一暗号鍵302で暗号化されているメッセージ鍵327を復元する（ステップ412）。この時、暗号化されているメッセージ326はそのままである。

【0063】受信者計算機311が受信者復号鍵312と暗号／復号装置314を用いて、同一暗号鍵302で暗号化されているメッセージ鍵327を復号し、元のメッセージ鍵317と同じメッセージ鍵328を得る（ステップ413）。暗号化されているメッセージ326をメッセージ鍵328と暗号／復号装置314を用いて復号する（ステップ414）。この復号したメッセージ330を受信者に対して出力する（ステップ415）。なお、本発明では、メッセージ鍵と復号鍵とを別物として説明したが、秘密鍵暗号を用いてメッセージを暗号化する場合には、同一の鍵となる。

【0064】

【発明の効果】本発明によると、送信者からサーバに送られるメッセージもしくはメッセージ鍵は、メンバが共通に持っている鍵で暗号され、さらにサーバの鍵で暗号されているので、サーバだけが復号できる。

【0065】また、メーリングリストから抜けてしまったメンバはたとえ、メンバ同一の復号鍵を持っていたとしてもアクセスできない。メンバが減った時には、メールサーバ計算機内部の変更だけで済み、メンバ送受信者の計算機の変更が不要になる。

【0066】また、メッセージもしくはメッセージ鍵はメンバ計算機だけが復号できる同一鍵で暗号されているのでメールサーバ計算機はアクセスすることができず、第三者による盗聴、情報の漏洩を防ぐことができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示すシステム構成図である。

【図2】本発明の第1の実施の形態の処理を示すフローチャートである。

【図3】本発明の第2の実施形態を示すシステム構成図である。

【図4】本発明の第2の実施の形態の処理を示すフローチャートである。

【符号の説明】

102…同一暗号鍵、103…サーバ暗号鍵、104、109、114…暗号／復号化処理装置、105、11

0, 115…通信装置、107…サーバ復号鍵、108…受信者暗号鍵、112…受信者復号鍵、113…同一復号鍵。

【手続補正2】

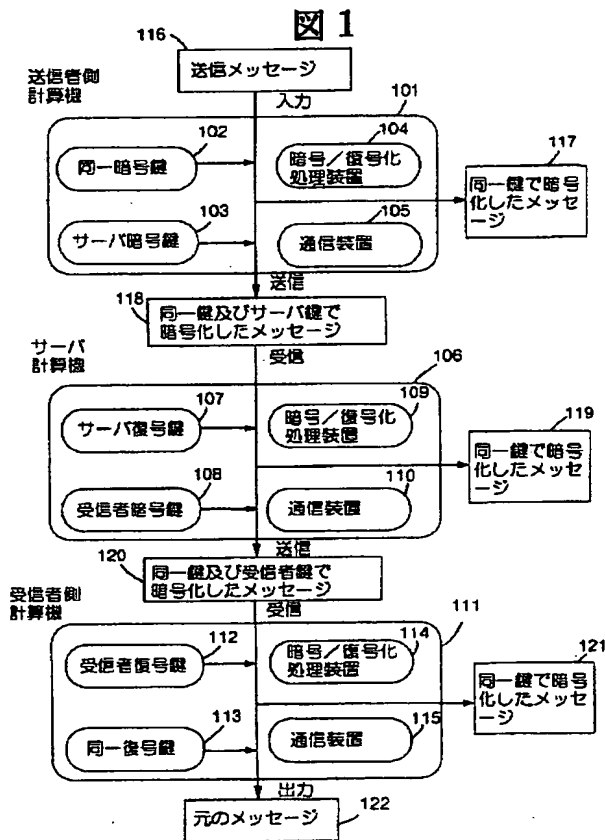
【補正対象書類名】図面

【補正対象項目名】全図

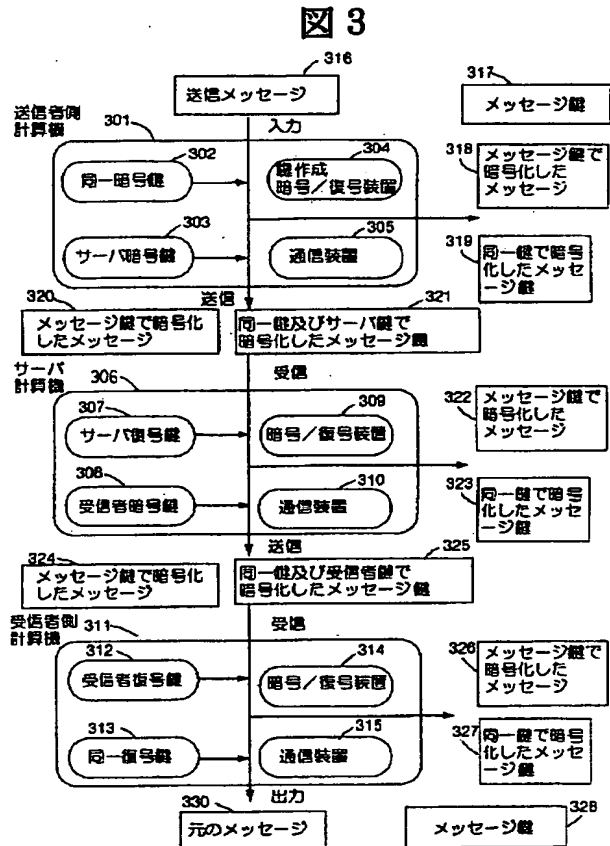
【補正方法】変更

【補正内容】

【図1】

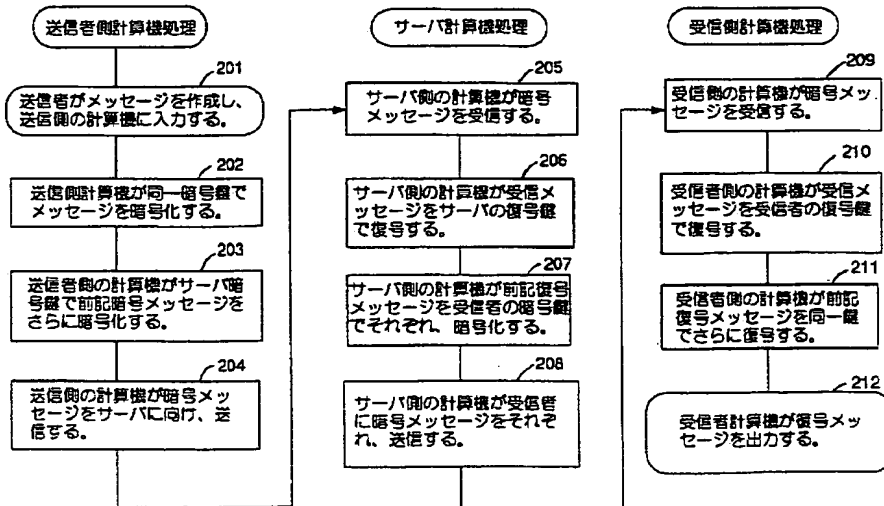


【図3】



【図2】

図2



【図4】

図4

